6. What are the types of IDOR?

Insecure Direct Object References (IDOR) can appear in different forms, each affecting a system in unique ways. Here are the primary types of IDOR vulnerabilities:

1. Horizontal IDOR

- **Description**: In a horizontal IDOR attack, a user accesses the resources or data of another user with a similar permission level.
- **Example**: Suppose two regular users have unique profiles, identified by `user_id`. If User A can change their `user_id` parameter to access User B's data, that's a horizontal IDOR.
- **Common Use Cases**:
  - Accessing other users' personal profiles.
  - Viewing other customers' order details in an e-commerce system.
  - Reading private messages not intended for the attacker.

2. Vertical IDOR

- **Description**: Vertical IDOR occurs when a lower-privileged user (like a regular user) accesses resources or functionalities meant only for higher-privileged users (like administrators).
- **Example**: If a regular user changes a parameter to access an admin panel or sensitive data restricted to higher privileges, it's a vertical IDOR.
- **Common Use Cases**:
  - Regular users gaining access to admin-only endpoints or features.
  - Editing permissions that should be restricted to administrators.
  - Viewing system logs or sensitive configuration data.

3. Object-Level IDOR

- **Description**: This form of IDOR occurs when references are assigned to specific objects, like documents or records, and users can modify these references to access unauthorized objects.
- **Example**: An IDOR in an API that uses `document_id` in the URL (e.g., `/api/documents?document_id=123`) may allow users to access other users' documents by modifying `document_id`.
- **Common Use Cases**:
  - Document storage systems where documents are indexed with predictable IDs.
  - File-sharing services that expose file identifiers in URLs.
  - Systems with predictable identifiers, like invoices or tickets, that could be incremented to reveal other records.

4. Function-Level IDOR

- **Description**: A function-level IDOR happens when an application allows a user to perform actions meant for a different user role by exploiting identifiers.
- **Example**: Suppose an e-commerce app allows users to change their user role ID in the URL or parameters. If a regular user modifies it to match an admin role, they might gain access to administrative functions.
- **Common Use Cases**:
  - Changing user roles or permissions.
  - Triggering restricted actions like account deletion or password resets for other users.
  - Performing unauthorized actions that are usually restricted to specific users or roles.

5. Multi-Step or Chained IDOR

- **Description**: In some applications, IDOR vulnerabilities can be exploited through a series of actions or steps. Attackers chain multiple IDOR vulnerabilities to achieve their goal.
- **Example**: An attacker might first use IDOR to gain access to a specific user's profile, then use another IDOR flaw to access or modify sensitive data within that profile.
- **Common Use Cases**:
  - Accessing and then editing user data.
  - Combining multiple IDOR vulnerabilities to gain a higher level of access or extract more data.
  - Exploiting different steps in a multi-step workflow, like a payment process.

Summary of IDOR Types

IDOR Type	Description	Examples
Horizontal	Accessing resources of another similar user	Viewing another user's profile, reading private messages
Vertical	Accessing resources meant for higher privilege levels	Regular user accessing admin functions
Object-Level	Accessing different objects within the same level	Modifying `document_id` to access other documents
Function-Level	Performing restricted actions by changing roles	Changing user role to admin to gain additional permissions
Multi-Step/Chained	Exploiting a sequence of IDOR flaws	Combining profile access with edit permissions to modify sensitive data

Each type of IDOR can lead to serious security issues, depending on the sensitivity of the data or actions the attacker gains access to.